

38. The method of claim 36 wherein any one or more of a collection of user interaction devices and methods may be used to effectuate commands and signals in a document generation and signature process,

whereby the action of a computer mouse, user's voice command, pressing of a key on a keyboard or keypad, pressing of a stylus on a pad, or of a stylus or finger on a screen, or any other method of user interaction can be employed to effectuate signature transactions at a server computer from a client user.

39. The method of claim 36 wherein the server's encryption device consists of a unique encryption key, generated from a symmetric cipher using the unique document identifier of a document as the character input of a password for generation of the key,

whereby each document to be signed is encrypted with a unique symmetric key, and whereby a cryptotransformation of a document involving the application of such key constitutes its signature.

REMARKS -- General

By the above amendment, Applicant has amended the title to emphasize the novelty of the invention.

Also, applicant has clarified the post office address by a statement of postal address which is signed and enclosed.

Applicant has complied with the direction of the examiner to include the legend "Prior Art" on figure 1. A revised copy is attached.

Applicant further requests leave to amend figure 3 to substitute for the legend "Unique Signety™ token" the correction "unique document identifier", in accordance with the amended claims.

The specification has been amended so that the summary precedes the description of the drawings, as directed by the Office Action. A substitute specification, which corrects certain

typographical errors that were noted in the Office Action is enclosed. It further amplifies the matters as set forth in the Office Action regarding the subject matter of templates, boilerplate, and digital wrapper as set forth in the Office Action. A statement accompanying substitute specification is also enclosed. A substitute specification mark-up is also enclosed. All claims have been rewritten to define the invention more particularly and distinctly so as to overcome the technical rejections and define the invention's patentability over the prior art.

Section 112 Objections and Rejections

The specification has been rewritten in light of the objections and rejections, which applicant respectfully requests be reconsidered in light of the changes.

With regard to wrapping, the substitute specification now includes a specific description as set forth on pages 7 and 8 thereof together with boilerplate and templates. With regard to symmetric encryption, the substitute specification now includes description on page 10 of alternative embodiments.

In light of the changes to the specification as contained in the substitute specification, applicant respectfully requests the examiner to reconsider the rejection of the claims, which have also been amended.

Section 101 Rejections Are Overcome

Applicant respectfully requests the examiner to reconsider the rejections under Section 101 in the light of the rewritten claims directed to a computer program and the claims directed to a method and apparatus. The former claim 16 has been deleted in the amended claims, which are no longer directed to a computer program.

The Rejections on the Basis of Haber, et al. under Section 102 Are Overcome

The O.A. dated September 28, 2000 rejected claims 1, 3, 6, 9 and 16 pursuant to section 102 (b) as being anticipated by Haber et al. (5136647) and (5136646). Applicant respectfully

requests reconsideration of this rejection, as now applicable to the redrafted claims, for the following reasons.

As the Court stated in *Jamesbury Corp. v. Litton Industrial Products Inc.*, 756 F.2d 1556 (Fed. Cir. 03/12/1985),

Anticipation requires the presence in a single prior art disclosure of all elements of a claimed invention arranged as in the claim. *Soundsciber Corp. v. U.S.*, 175 Ct. Cl. 644, 360 F.2d 954, 960, 148 U.S.P.Q. (BNA) 298, 301, 149 U.S.P.Q. (BNA) 640 (1966).

The standard is not met on the basis of *Haber*. *Haber* (5136647) includes elements not present in the instant invention: These include: 1. creation and hashing of the document prior to submission for time stamping to the agency, 2. numbering of the authors, and 3. issuing a sequential receipt number, all prior to digital signature, and after signature, 4. sending the document to at least one other witness for further processing . See *Haber* (5136647), columns 6 – 8 and claims 1-12 by way of example. All of these steps are eliminated in the present invention. In *Haber* (5136646), similar steps are noted in columns 6 –8 except that a running concatenation of hashes is hashed anew as each new hash is added to the global result, which is also eliminated in the present invention. The elimination of these steps establishes the physical novelty of the invention over *Haber* (5136647) and *Haber* (5136646).

There are also elements in this invention which are missing from *Haber* (5136647) and *Haber* (5136646) and which independently establish the physical novelty of the present invention. Redrafted independent claims 20, 30 and 36 all clearly require a client-server relationship, which is not present in *Haber*, and dependent claim 23 requires the use of a data store which is also absent from *Haber*. In the redrafted claims, a unique identifier is involved with the document signature information, which is not a part of the *Haber* patents. In *Haber*, by contrast, the identifier is kept separate and apart from the original document whose date and time is to be proven. With regard to *Haber* (5136646), the instant invention uses a digital signature, which is absent from that invention. Also, independent claims 30 and 36 and the dependent claims 31 and 32 of this invention include document creation methods at the server, such as boilerplate and templates that users fill out, and form input devices for user input, and which result in

documents that can include formatting and structural tags to permit display and use by applications that require such tags. Further, dependent claims 28, 33 and 39 provide for the use of a symmetric cipher to sign, which is absent from Haber. Again, these differences establish the physical novelty of the invention over Haber (5136647) and Haber (5136646).

Accordingly, the applicant respectfully submits that the claims of this invention are not anticipated by Haber, and are patentable over Haber et al. (5136647) and (5136646) notwithstanding section 102(b).

Section 103 Rejections

There are a number of section 103 rejections. What follows is a discussion of the law that is applicable to section 103 rejections generally and is therefore useful with regard to each of the specific rejections.

The Court of Appeals for the Federal Circuit in *Northern Telecom Inc. v. Datapoint Corp.*, 908 F.2d 931 (Fed. Cir. 06/29/1990) ¶¶ 32-34 has stated:

It is insufficient that the prior art disclosed the components of the patented device, either separately or used in other combinations; there must be some teaching, suggestion, or incentive to make the combination made by the inventor. *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1143, 227 USPQ 543, 551 (Fed. Cir. 1985) (insufficient to select from the prior art the separate components of the inventor's combination, using the blueprint supplied by the inventor); *Rosemount, Inc. v. Beckman Instruments, Inc.*, 727 F.2d 1540, 1546, 221 USPQ 1, 7 (Fed. Cir. 1984) ("As this court has held, 'a combination may be patentable whether it be composed of elements all new, partly new or all old'" (citations omitted); *W. L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1551, 220 USPQ 303, 312 (Fed. Cir. 1983), cert. denied, 469 U.S. 851, 105 S. Ct. 172, 83 L. Ed. 2d 107 (1984) (individual references can not be "employed as a mosaic to recreate a facsimile of the claimed invention.")

....

As discussed in *In re Rothermel*, 47 C.C.P.A. 866, 276 F.2d 393, 397, 125 USPQ 328, 332 (CCPA 1960), the nature of the problem "which persisted in the art", and the inventor's solution, are factors to be considered in determining whether the invention would have been obvious to a person of ordinary skill in that art. See also, e.g., *Fromson v. Advance Offset Plate, Inc.*, 755 F.2d 1549, 1556, 225 USPQ 26, 31 (Fed. Cir. 1985) (the prior art must suggest to one of ordinary skill in the art the desirability of the claimed combination).

See also *In re Zurko*, 142 F.3d 1447, 1459, 46 USPQ2d 1691, 1701 (Fed. Cir.) (en banc), cert. granted, 119 S. Ct. 1816 (1999)(on other grounds):

[T]he Board impermissibly used hindsight to arrive at the claimed invention. See *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 USPQ 303, 312-13 (Fed. Cir. 1983) ("To imbue one of ordinary skill in the art with knowledge of the invention in suit, when no prior art reference or references of record convey or suggest that knowledge, is to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against its teacher.

With these principles in mind, a request is made to reconsider the various Section 103 rejections, each of which is discussed below.

The Rejection of Claims 14, 15, and 17 on the basis of Haber (5136647) or (5136646) are overcome.

The O.A. rejected former dependent claims 14, 15 and 17 on the basis of Haber. These claims included affixing a signature on a form by pressing a button (no. 14), providing information via a form that is presented by the server computer to the user's computer (no. 15) and providing information from a user to the server via a form (no. 17). The common theme of the claims and their rejection is the use of a form to effectuate certain user actions in connection with document generation and signature at the server computer. The rejections all cite Haber's timestamping authority as the basis for the rejection, and seem to assume without expressly stating it that the form is simply a means for effectuating a time-stamp with this invention. Thus, under the

reasoning of the rejections as applicant understands them, the dependent claims add nothing new to the invention and the rejection is based upon the underlying view of the time stamping invention of Haber as prior art.

The various claims have been rewritten as amended independent claims 20 a. 3 (user signature action), 30 (d)(e) and (g) and 36 (c), and dependent claims 31 and 32 (document generation through user input) as well as independent claim 36 (f) and dependent claims 24 and 38 to define patentability over these references. Applicant requests reconsideration of this rejection as now applicable to amended claims cited above for the following reasons.

The novel features of the present invention produce new and unexpected results and hence are unobvious and patentable over these references. The amended claims each involve a client-server relationship, which is missing from Haber. A client server relation integrates processes between two or more machines acting as parts of a single entity, and creates a division of functions between the client and server in a distributed architecture which Haber did not foresee, suggest or teach. Haber did not envision or foresee in this client-server environment that a plurality of clients each ***sign their own names*** to documents using a server's encryption facilities, as in the present invention. In Haber, the digital signature generated by the time stamping service is not intended or considered to be the verifiable signature of the authors themselves. The digital signature in Haber is not related to the identified or authenticated authors, but rather to the date and time that a document was presented to the agency for verification, to allow authors to contact other authors for the purpose of confirming a sequence of date and time stamps and proving the truthfulness, in terms of chronological accuracy, based upon the combination and sequence of time-stamps of more than a single author. There is no suggestion in Haber that the signature of the server in the Haber invention can be used or adapted for the distinctly different purpose of creating verifiable, binding signatures for client users that cannot be repudiated by them, and doing away with encryption keys, digital certificates and writing tablets and stylus' on the client machines for this signing purpose, or suggesting the use of symmetric signature means, as in claims 28, 33 and 39 of this invention.

In fact the reissued Haber patent expressly teaches away from these purposes.

Reissued Haber No 34,954, included with the OA clearly states in column 4, line 35 that "So effective is such a sequential fixing of a document in the me stream that the TSA signature could be superfluous in actual practice." This de-emphasis of the importance of the digital signature clearly indicates that signature of a user's identifier and a document's identifier was not a purpose of, nor was contemplated or suggested by, Haber's invention.

Although Haber teaches the use of time stamping, it is for the purpose of establishing the date and time that a document was submitted to the agency for stamping, as later proof of its existence as of and prior to that time. That is very different from the present invention, where the date and time is used as a way of providing a unique identifier for the signature of the client itself. No two seconds in time are identical. No two persons can operate a device at the same IP address at the same instant of time. Therefore, using the IP address and the date and time of the server as in the preferred embodiment of the substitute specification and the original specification provide a unique characteristic to distinguish each signature transaction from each and every other signature transaction, even if only one asymmetric private key at the server is used successively by the same client user operating a computer at the same IP location to create successively signed documents or files. Each signature will be unique and uniquely verifiable because the date and time component of the signature will be different for each document or file. Where a symmetric cipher is used, each key used to encrypt a document will necessarily be unique for the same reason. This is totally unlike Haber, where authors are given numbers that are not globally unique but rather correspond to a numbering scheme of one agency only, and without reference to the possibility that two agencies could assign the same number to two different authors or documents. That is because it is the actual date and time chronology that is important in Haber, and not the uniqueness of the identifiers that are important. Haber thus does not suggest, foreshadow or teach the art of this invention, which represents a new and different use. There is no suggestion in Haber of using the server's date and time, in conjunction with the IP address of the client, to create a globally unique identifier for a signature transaction created in a client-server relationship. The use of the date and time in this invention is an unexpected result and benefit not anticipated by Haber.

As a corollary, the purpose of the button of the former claim 14, now amended claims 20 a. 3, 24, 30 (g) and 38, is to emphasize the expression of intent by the signer to adopt the contents of the document irrevocably as his, her or its own and be bound by it, a factor which is notably missing in Haber, whose technology is directed to a different purpose.

With regard to former claims 15 and 17, now amended claims 30 (d) and (e), 31, 32, 34, 36 (c) and 38, the form information is for the purpose of obtaining user input in a document creation process at the server, not simply to assist in a scheme to establish priority in time of certain information, as in Haber. Haber does not discuss the creation of a document through templates that are filled in with information provided by a user. Document creation and signature at the server are both important elements of this invention. The amended claims establish a method for creating a document for signature at the server which includes either or both boilerplate and blank items for filling in the by the user and signature of the combination as a document which cannot later be repudiated by the signer. Haber mentions nothing about document generation through the agency at a server as part of his invention and he makes no claim to the document creation aspect of this invention. Haber should not therefore not be determined to have envisioned the amended claims of this invention.

Because Haber does not even faintly suggest the creation of documents at a server for the purpose of signing them using the server's encryption key, or user interaction from a client for such purposes, and at a server without a need for client-side certificates or signature tablets, amended claims 30 (d) and (e), 31, 32, 34, 36 (c) and 38, formerly dependent claims 15 and 17, are not suggested by Haber, and this invention is patentable over Haber.

This invention is directed to the prior art of digital certificates and signing tablets for use at client machines, and Haber does not discuss, assume or envision anything related to such prior art. One of the unexpected results of the present invention is the enhanced privacy of the signers. Digital certificates from certification authorities under prior art to establish non-repudiation of signatures can also be used by marketing firms and governmental agencies to track users as they navigate over the Internet and collect information about their movements and preferences. With the removal of all certificates from client devices in the instant invention, the possibilities for

such surreptitious surveillance are removed. There is no suggestion of this result or benefit in Haber.

Similarly, with client side keys and certificates, unlike the present invention, private keys can be stolen from client side machines, used to impersonate identity and create opportunities for theft of personal assets. With the removal of all keys and certificates from client side machines with the present invention, opportunities for identify theft are decreased. There is no suggestion of this result or benefit in Haber.

Private keys cannot be shared using the prior art without creating a security breach, but industry experts agree that such sharing is probably inevitable, creating an insecurity that cannot be remedied through technology. With this invention, there is no possible sharing of client side private keys because they are removed and replaced with encryption services of the server, which are regulated and controlled in terms of sharing by the server through the client-server relationship. There is no suggestion of this result or benefit in Haber.

The redrafted claims 20 a. 3, 30 (d)(e) and (g) and 36 (c), dependent claims 31 and 32 as well as independent claim 36 (f) and dependent claim 38 more clearly spell out the distinctions and overcome the prior rejections, which the examiner is respectfully requested to reconsider in the light of the changes.

In light of the request, applicant further submits that the invention has received recognition and of commercial success, as set forth in the accompanying affidavit of John Messing.

Section 103 Rejections on the basis of Haber and Micali Are Overcome.

The O.A. dated September 28, 2000 in paragraph 33 and 34 rejected former dependent claims 4, 7, 12, and 19, now amended claim 26 under section 103 as being unpatentable over Haber et al. (5136647) and (5136646) in light of Micali. Applicant respectfully requests reconsideration of this rejection, as now applicable to the amended claims, for the following reasons.

1. With regard to paragraph 33 of the O.A., the identifier which Haber 5136647 discusses in column 6, lines 8-15 is different from the authentication elements of this invention. Haber's identifier is not used later to authenticate an author's identity and prove he or she is in fact the individual who prepared and signed a document as though with his own signature. It is simply a way of labeling the source of the data so that commonly derived hashes, which are the crux of that invention, can be reconstructed by the various authors of different documents to show there has been no possible backdating of any receipted times. In this invention, where an authentication method is used, it establishes the identity of the signer at a later time after enrollment based upon the invention's authentication mechanism. That is an entirely novel purpose and result.

2. With regard to paragraph 33 and 34 of the O.A., the rejection on the basis of obviousness has been addressed with respect to Haber 5136646 and 5136647 with regard to section 102, and the comments previously made with regard to Haber are incorporated by reference.

3. The reference to Micali 5666420 in paragraph 34, with all due respect, is a misreading which results from a juxtaposition of two sentences which when read together create an unintended and unwarranted conclusion. Micali does not actually say that **countersigning** is done to prevent a maliciously prepared message. He says rather that **signing** by Bob is done to prevent a maliciously prepared message. Under Micali, Bob signs the encrypted message z from Alice whether Alice also signs it or not. See column five, the bottom portion thereof. Therefore, the use of the word "countersign" in the first of the two quoted sentences of Micali denotes simply that if Alice optionally signs the value of z, which is done so that Bob can be sure that z really came from Alice, then Bob will sign secondly, after verifying Alice's signature. No further function or mechanism related to Micali's invention is intended by the word "countersign" and no suggestion or foreshadowing about countersigning or re-signing as in the redrafted dependent claim of the present invention can be inferred. In this invention also, the same person signs twice as additional proof of intent and authentication of the original and only signer. In Micali, two different people sign. There is no relationship between the inventions and Micali, with Haber, does not suggest this one.

4. Micali's invention does not anywhere actually claim a countersignature. It does not teach or claim the value of a countersignature as used in this invention.

5. Micali's invention involves a system to allow a person who tenders something of value to obtain a signed receipt for it. This is applicable to contracts and certified email. Micali wants to be able to create a simultaneous exchange electronically. For this purpose a trusted third party can be called in for the unusual case where one party refuses to release the consideration it owes to the other. Nothing is suggested about creating and countersigning transaction records, documents, filings, messages or other communications electronically by a single signer for the purpose of preventing non-repudiation by a signer or detecting message alterations, as in this invention.

6. In Micali's invention, which assumes a certified email transaction in the preferred embodiment, Alice sends a message to Bob and wants a receipt signed by Bob for it as a condition of him receiving it. In order to oblige both parties to perform, Micali postulates a third party, PO. All three have encryption keys. Alice first encrypts the message with Bob's public key, encoding it, and then encrypts that encryption with PO's encryption key, producing z. Bob has his decryption key, but not the post office's. He cannot decrypt z himself. Upon the receipt of z, he digitally signs it and sends it to Alice. Alice sends him the message a second time, encrypted this time only with his public key. Bob can decrypt the message with his private decryption key, without any further help. Alice winds up with the signed receipt and Bob winds up with the message. Bob can check to make sure it is the same message that was incorporated in z to begin with by re-encrypting the final decrypted message received by him with first his public key, as did Alice, and then the PO's public key, reproducing the value of z. If z as sent by Alice equals the reconstructed z, the message is authentic, ***without the use of any digital signatures***. Bob's signature on z is not required for any purpose other than furnishing a signed receipt to Alice. It does not enter into the workings of the invention otherwise. Alice's signature is mentioned as a refinement so that Bob can be sure that z really came from Alice, but this is not central to the invention and is treated as secondary by Micali, whose claims do not reference the countersignatures of the parties. A second signature of the signer in this invention is wholly new and novel in light of Micali and is patentable over it and Haber in combination.

7. If Alice refuses to provide the second encrypted version of the original message, Bob can go to PO to get it to unlock *z* and release the message as it was encrypted only with his public key, which he can decrypt with his own private key. PO sends the signature to Alice, and the parties both get their due.

8. In the present invention, nothing envisioned by Micali is remotely involved. Under the Uniform Electronic Transactions Act, which is referenced in recent federal legislation, many kinds of technologies can be used to create legally binding electronically signatures, including voice signatures, all of which dependent claim 26 encompasses. Micali, on the other hand, only concerns digital signatures based on asymmetric encryption, including the passing, secondary reference to a countersignature. Therefore this invention is new and novel when considered in light of Micali, and claim no. 26 is patentable over Micali and Haber.

9. In all other embodiments of this invention, authentication of a signer takes place prior to affixing the server's signature. In the embodiment involving two successive signatures of a sole signer, the server first assembles and signs the transaction record, document, filing, message or other communication without necessarily authenticating the signer beforehand. The signer reviews the digitally signed transaction record, document, filing, message or other communication for correctness before finally approving it. If acceptable, the signer resigns locally with another signature device. This has the advantage of allowing the signer to see the finally assembled transaction record, document, filing, message or other communication bearing a first digital signature of the server before finally affixing a final, intended-as-binding signature. It is an option that eliminates any possibility, no matter how remote, of machine error, abuse, or other alteration in the process of marrying the template information with the user input provided by the signer. It has the disadvantage of requiring two signatures and more complex processes, but the advantage of eliminating any possibility of error or mishap in the final approval process by delaying the final signature until a proposed transaction record, document, filing, messages or other communication that is already digitally signed has been presented for re-signature to the signer. Therefore this invention is new and novel when considered in light of Micali, and claims 26 is patentable over Micali and Haber.

10. Neither Haber nor Micali refer to each other or even seem to be aware of each other's inventions. There is nothing to suggest that they can be combined practically, and no attempt has ever been made to do so. They teach contrary to each other in that Haber teaches hashes and signatures while Micali teaches encryption, not signatures. Taking a little from one and something from the other to claim prior art is contrary to the teachings of the cases previously cited. There is nothing in Haber or Micali that teaches the present invention, includes its elements, or suggests it.

The Supplemental Authority is not prior art which must be overcome.

Applicant has submitted Supplemental Form PTO-1449 Substitute transmitting a publication with a first publication date of April 7, 1997 entitled Baum and Ford, Secure Electronic Commerce (1997) pp. 332-3, 352. The publication discusses the use of a trusted third party's key by signers in lieu of client side certificates. However unlike this invention, the publication's embodiment assumes the creation of a document or message at a user's machine and by footnote 35 specifies that authentication of a signer to the trusted third party's key exclusively must be by public key cryptography or Kerberos authentication. By contrast, in this invention, in the preferred embodiment a document is created at the server, and not at the user's machine, and authentication is optional with regard to all embodiments. Where authentication is used, the method of authentication is not limited exclusively to public key cryptography or Kerberos as in the publication. Where authentication is used in this invention, acceptable methods may also include a username and password, or biometric identifier, none of which is mentioned as suitable in the publication's criterion. Furthermore, this invention does not require any authentication in certain embodiments but instead in such cases relies upon an identifier assigned to a document, without other means of authentication, which identifier in one embodiment may be constructed from the user's IP address and the server's date and time value, with a credit card authorization from a credit card provider if this is available, without any additional information such as would be provided by public key cryptography or Kerberos mechanisms. Furthermore, this invention can use symmetric ciphers to sign, which method is totally absent from the furnished publication. Thus, it is apparent that the furnished publication is not prior art as to the present invention, which provides a new and novel approach to document creation, authentication and a client-server signature mechanisms.

Conclusion

For all of the above reasons, applicant submits that the specification and claims are now in proper form, and that the claims all define patentability over the prior art. Therefore, applicable submits that this application is now in condition for allowance, which action is respectfully solicited.

Conditional Request for Constructive Assistance

Applicant has amended the specification and claims of this application so that they are proper, definite and define novel structure which is also unobvious. If, for any reason this application is not believed to be in full condition for allowance, applicant respectfully requests the constructive assistance and suggestions of the Examiner pursuant to M.P.E.P. Sections 706.03(d) and 707.07(j) in order that the undersigned can place this application in allowable condition as soon as possible and without the need for further proceedings. Alternatively, if the examiner agrees that patentable subject matter is presented but does not feel that the present claims are technically adequate, applicant respectfully requests the examiner to write acceptable claims pursuant to MPEP 707.07(j).

Very respectfully,


John H. Messing
Applicant Pro Se

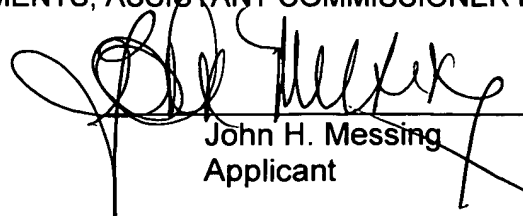
6571 N. Silver Smith Place, Tucson, AZ 85750

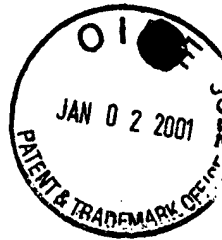
Tel.: (520) 327-7750 or (520) 529-3275

Fax: (520) 325-1087

Certificate of mailing: I certify that on the date below this document and referenced attachments, if any, will be deposited with the U.S. Postal Service as first class mail in an envelope addressed to : "BOX NON-FEE AMENDMENTS, ASSISTANT COMMISSIONER FOR PATENTS, WASHINGTON, D.C. 20231."

December 28, 2000


John H. Messing
Applicant



In the United States Patent and Trademark Office

Serial Number: 09/081,872
Appn. Filed: 05/20/98
Applicant(s): John H. Messing
Appn. Title: Electronic Signature Program
Examiner: Douglas J. Meislahn
Group Art Unit: 2767

December 28, 2000

Tucson, Arizona

Substitute Specification Mark-Up

Assistant Commissioner for Patents
Washington, District of Columbia 20231

Sir:

With regard to the substitute specification the following is a markup as rendered by the word processing program Microsoft Word 2000 after comparing the original and substitute markup filed herein:

Patent Application of
John H. Messing
for an

ELECTRONIC SIGNATURE PROGRAMMETHOD

Cross References to Related Applications

None.

Background -- Field of Invention

This invention relates to creating and verifying between computers and on computer networks electronic signatures for electronic documents, filings and transaction records.

Background -- Description of Prior Art

An electronic document, legal filing or record of an electronic commercial transaction requires a way to authenticate the parties. Because handwritten signatures on paper have performed the authentication function traditionally, and electronic documents do not allow for this physical method of authentication, electronic substitutes must be found.

Until now, two principally different systems have been devised for "signing" electronic documents, but each has one or more significant drawbacks.

One such system, based upon the invention shown in U.S. Pat. 4,405,829 to Rivest et al. (1983) is based upon ~~uses client-side digital signatures and certificates created through the technology known as of "asymmetric encryption." In this technology, a user generates two mathematically related numbers that are similar to very long passwords, called keys. The so-called private key remains with the issuing user. The other key, denominated the public key, is distributed by the issuer to others for the purpose of verifying communications. The keys are related, but they are not identical. They perform reverse roles. One is used to encrypt information, and the other to decrypt it.~~

Electronic communications are signed, generally with the private key, in a two step process. First a digest of a message is created with a one way hash function, and then the hash function is encrypted using the private key. The authenticity of the message and its contents can be verified by a recipient as being authentic and sent from the signing party through testing of the message using the public key. Either an altered message or fraudulent sender will be detected by a computer possessing the proper software, the public key, and the digital certificate of the signer. If the message has been altered or the signer did not use the proper private key, the message will be detected as false. This method is useful for electronic authentication.

~~However, this method of authentication also requires a massive infrastructure for key management and verification by trusted third parties, called certification authorities, who~~
For more secure types of authentications, certification authorities typically check the

~~identities of key holders,~~holders and issue certificates to ~~them verifying~~verify that they belong to the party who is identified as the holder of the key ~~pair, and~~pair. They maintain lists of active and revoked certificates for use by relying third parties. Determination of authentication requires not only a check of the digital signature on the message, but also of the status of the certificate identifying the signer, which involves accessing the certificate authority and knowing how to check the lists of revoked and suspended certificates. The investment to create and operate a certification authority is considerable.

~~Another difficulty with this technology is that private~~Private keys are also susceptible to theft from the computers or devices where they are stored, and when stolen, can be used to commit fraud with virtually no detection until the certificate of the user is revoked by the certification authority with respect to that particular corresponding public and private key ~~pair.~~

pair. Private keys can also be compromised by sharing the passwords used to access them.

The creation and maintenance of the certification authority infrastructure requires a massive investment in equipment and personnel that results in a relatively high cost to the end user where suitable means are adopted by the certification authority to verify the true identity of a holder of a private key before issuance of a digital certificate to the alleged owner of the key.

Furthermore, in business and legal settings where both parties are required to electronically sign documents, filings or transaction ~~records using their respective private keys and digital certificates, and they are located in or claim citizenship of different legal jurisdictions or countries, there is a possibility for uncertainty or actual~~records. digital certificates may be more secure and expensive than the realities of the transaction warrant, while in other settings, the protections may not be sufficient.

~~conflict in the laws applicable to the transaction. In some countries, users may be required to give copies of the keys to the applicable governmental authority upon pain of punishment. This requirement may compromise the privacy and security of the electronic signatures. Where different legal regimes are involved, such uncertainty or conflict may actually impede the use of the electronic signatures for fear by participants of legal attacks~~

~~from overzealous authorities or corrupt ones, depending on the reputations of the countries involved and their political regimes.~~

PenOp, U.S. Pat. No. 5,554,255(1994), and continuation serial number 298,991, U.S. Patent 5,647,017 (1997) and related patents cited therein, adopts a completely different approach to electronic signatures. It uses digital drawing tablets on a client machine as a basis for digitally capturing a handwritten signature, and then through software stores certain signature characteristics which identify the dynamic movements of the writer's hand as it moves the stylus on the tablet during signature creation, in addition to the image of the signature on the tablet. This stored information is then compared to a subsequently generated signature to determine if the signature is authentic. If a hash function is captured, digested, and linked to the document, this approach, like the "digital signature" approach of the "asymmetric encryption" can determine any changes that have been made to the document since the signature was applied.

This "dynamic signature" approach avoids the massive infrastructure of the "public key encryption" certification authorities, and the problem of conflicting legal regimes applicable to electronic signing of documents in an international or multi-jurisdictional setting, but it requires the provision of a digital drawing tablet and stylus at each computer workstation where signature is to be accomplished, as well as the related software, which can be a significant system-wide item of cost. In addition, traditional forensic analysis applicable to handwritten signatures does not yet apply to electronic signature analysis, and it may be some time, if ever, before the legal forensic community becomes adept at dynamic signature handwriting analysis. Because there is no way at present for expert analysis of dynamic signatures, the ability to authenticate signatures is arguable at best.

~~In addition, these technologies are mutually exclusive, in that one cannot incorporate the other, and it is not possible to use them together under prior art.~~

Objects and Advantages

Accordingly, several objects and advantages of the invention are to provide a new type of electronic signature that does not depend upon the massive certification authority infrastructure of digital signatures on multiple client machines based on asymmetric encryption or the hardware and software investment of dynamic signatures; further that it uses only one a signature key of the a server computer located in and subject to the jurisdiction only of the political authority of the server computer, rather than many signature keys of many client computers, further that it automatically incorporates information about the signer and generates and affixes a date and time stamp as proof of those parameters parameter taken from the server's clock as evidence of identity at the time of the signature; further that it eliminates the need for development of a discipline that does not yet exist, namely, the forensic science of electronic handwriting analysis; and that further allows for the use by incorporation of the other two forms many types of authentication into its system, as well as others that exist or may emerge in the future.

Still further objects and advantages will become apparent from a consideration of the ensuing description and accompanying drawings.

Drawing Figures

Fig. 1 shows authentication as a means of access by a web browser to a web server.

Fig. 2 shows how a web server "parses" or separates out for storage certain information transmitted by a web form page.

Fig. 3 shows the creation of the signature from database submission information and the system clock.

Fig. 4 is a representation of the machine process whereby the computer takes the signature token, wraps it in a digital wrapper, and signs it with the server's private key.

Fig. 5 is a representation of a web page as shown to the user which contains the signature button for signing the document.

Summary

In accordance with the present invention, an electronic signature program is described for the creation, monitoring, and verification of an electronic signature generated by the interaction between two computers, one a client and the other a server, for the signing of documents, filings or transaction records without the need for an expensive and massive infrastructure of certification authorities and the complexities of installing and using digital certificates, without generating conflicts between applicable legal regimes in an international or multi-jurisdictional setting over regulation of encryption software, and/or without requiring hardware tablets and associated computer software. This system further is able to incorporate other existing technologies of prior art designed to authenticate users to a server computer and ones not yet available or existing.

Drawing Figures

Fig. 1 shows authentication as a means of access by a web browser to a web server. While only certain transactions may require authentication, all users are identified at a minimum by unique network location (IP address).

Fig. 2 shows how a web server "parses" or separates out for storage certain information transmitted by a web form page.

Fig. 3 shows the creation of the signature from database submission information and the system clock.

Fig. 4 is a representation of the machine process whereby the computer takes the signature token, wraps it in a digital wrapper, and signs it with the server's private key.

Fig. 5 is a representation of a web page as shown to the user which contains the signature button for signing the document.

Description – Figs. 1 to 5

The electronic signature is affixed between computers over the Internet. Figure 1 depicts the initial contact between an Internet client user and an Internet server. This is accomplished by an ordinary web browser. Users are identified. A method for authenticating users allows the additional option to screen out unauthorized users (fig. 1, no. 12). To access the signature device, users must pass the authentication gateway. Where unauthorized users are to be excluded, many different systems of screening out unauthorized computer users can be utilized, including but not limited to digital certificates to users from trusted third parties, previously issued passwords, stored and verifiable dynamic signatures, credit card authorizations, retinal scans and other authentication methods, without limitation. Unless the system is open to all users, unauthorized users are rejected by the system using the authentication system. If the system is open, the authentication mode is universal, and all users are permitted to create electronic signatures, using identifiers only.

Information is collected from the users as shown in figure 2, (no. 14). It is transmitted for the purpose of (no. 15), parsing (separating out discrete information supplied by the user upon submission of a web page form that is specific to a filing, document or transaction)(no. 16) and storage of the information on the server computer (no. 17).

Creation of the signature is depicted in figure 3. In the preferred embodiment, the server has captured the unique network element parameter of a signer, and where available, a credit card authorization number from a card processor. Where authentication on the basis of stored identity criteria, such as a digital certificate, username and password, or biometrics is involved, alphanumeric elements, appropriate symbols or abbreviations can be used to represent these. Other user identifier elements are known to those skilled in the art and may include a legacy application that has developed a user identifier system. Certain information from the user elements (no. 18) are combined with the date-time

stamp parameters of the server's system clock (no. 19) to create a unique-Globally Unique Identifier (GUID) from the blend of the components. (no. 20). This combination also permits a date and time stamp to be incorporated into the signature.

Figure 4 demonstrates how the signatureGUID is encapsulated in the digital signature of the server computer. An active X (com) object or other applications programming interface (API)(no. 23) at the Internet server creates a digital wrapper (no. 24) and communicates with the signature program of the Internet server to sign the information (no. 22), including GUID, contained in the signature (no. 21) with the server's private key. Once the signature is thus encapsulated and digitally signed, it is included in an automatically generated email message (no. 25). It is sent to the user at the email address that the user self-reported to the Internet server initially.

The digitally signed wrapper ensures that the information included in it, including transactionGUID particulars, date and time stamp, and electronic signature cannot be altered after the fact without such change being detectable through software.
software.

The digitally signed wrapper also permits signer-supplied submission information to be inserted into a document for signature as part of a transaction template, which may include standard terms applicable to the class of transactions. The template may simply be a blank (structure only) document, to be filled in completely by the user, or it also may include "boilerplate", meaning standardized language that is intended to remain in the document. Boilerplate is commonly associated with legal, financial, real estate and mortgage phrases and provisions that are intended as inalterable in the document finalization and signature process. For example, it can include standard terms for purchase orders. For example, it can include notices and averments to governmental regulatory bodies. For example, it can include electronic credit card charge slips. By putting the boilerplate terms and conditions at the server and incorporating them as a template that cannot be modified by a signer, unauthorized pre-signature modifications are prevented. For example, in an extreme example, the template located on the server consists completely or almost entirely of boilerplate language that the signer is expected to accept and sign or reject without adding,

modifying or inserting any information specific to the signer or transaction. For example, the transaction template may be used as an envelope for the transmission and routing of one or more documents or files that are to be annexed. Any of the documents and files to be annexed can also be signed using this invention.

In a normal transaction, assuming a template consists of text *a, b, c* and more text *e, f, g* and still more text *i, j, k*; with spaces that a user fills in with transaction specific information *d* and *h*; then by way of illustrative example, the digital wrapper which is assembled for the signature at the server consists of $abc + d + efg + h + ijk + \text{GUID}$.

As one skilled in the art can appreciate, the GUID may appear in the document, in a detached signature, in a database record, in a cookie on a client user's machine or as part of the signed file information. The template can also include formatting and structuring information so that the relying party receives a document that can be read using conventional programs and methods. For example, the relying party may want to have the transaction in a word processing format. For example, the relying party may want to have the document include mark up tags common to and from such programs and languages as Hypertext Mark Up Language (HTML), Rich Text Format (RTF), Standard General Markup Language (SGML) or Extensible Markup Language (XML), and commonly used word processing formats. For example, the relying party may want to have a particular stylesheet associated with a document to preserve its layout as well as text and require the signer to sign this presentation formatting as well. By putting the templates and encryption keys on the server, and exposing the methods and properties of signature applications at the server, inconveniences caused by the complexities of using keys and certificates by non-IT professionals, and incompatibilities between operating systems and environments of the various signers' and relying parties' computers are also avoided.

Return of this information to the individual who signed the information is a receipt that is proof of the transaction, the electronic signature, and the transaction content.

If the email address is non-existent, intermediate mail server computers usually alert the server via a failed email message that the message was undeliverable. Such a message also serves to warn the server computer that a fraudulent transaction may be in progress.

Figure 5 depicts the mechanism for actually invoking the signature device, as viewed by the user. A simple button (no. 23) is clicked by the user, coupled with a clear warning (no. 24) of the consequences of clicking the signature button. Once the button is clicked, the electronic signature feature is ~~enabled~~.

enabled. Other means of user interaction with a machine besides the clicking of a button will be evident to one skilled in the art, and may include by way of examples a voice activated command, the pressing of a button on a keyboard, the use of a stylus or a finger on a screen, or a button on the remote control device for a television.

If the email receipt containing the electronic signature is received by the signer, that individual optionally may be required to countersign the receipt digitally (preferably using asymmetric encryption) and then to return the resigned message back to the server computer for storage and as further proof of receipt and authentication. This receipt at the server computer proves that the user actually received the electronically signed message, and the digital signature can be stored at the server as a further guarantee of message ~~authenticity~~.

authenticity. As one skilled in the art will realize, the example of email transmission is one of many possible ways of transmitting the digitally signed document from the server to its destination. Other examples include the saving of a web page of information directly from a browser to a hard drive, or the downloading of a document from one machine to another.

Conclusions, Ramifications, and Scope

Accordingly, it can be seen that the above system allows client computer users to sign electronic documents, filings and transaction records submitted to ~~another~~ a server computer as though with pen and ink on paper, without any additional hardware or software apart from an Internet web browser. The signature program reduces the need for a massive infrastructure investment of certification authorities by relying solely upon the

digital certificate of the server computer, without any similar requirement that the signing party obtain a separate digital certificate, unless optionally required for receipt signing purposes. ~~The program eliminates certain legal problems that may arise from attempts by multiple legal regimes to regulate encryption features of asymmetric encryption program, through key recovery programs, since only one key, that of the server computer is involved, and only one legal regime will likely be entitled to regulate the server. The~~ program method is able to make use of other current and future technologies for computer user authentication systems, and is suited for the Internet and other computer networks.

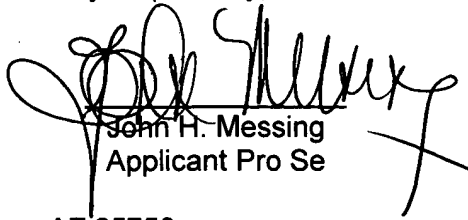
Although the description above contains much specificity, this should not be construed as limiting the scope of the invention but as merely providing illustrations of some of the presently preferred embodiments of this invention. Various other embodiments and ramifications are possible within its scope. For example, ~~and not by way of limitation other unique system information of the server can be used in addition to or instead of the system clock to generate a unique signature token. Similar, the signature and the filing, document or transaction record to be signed and be digitally wrapped and signed using techniques other than asymmetric encryption.~~ GUID, which may also be encrypted.

Modification within the spirit of the invention will also be apparent to those skilled in the art. For example, electronic processes may sign as client users on behalf of individuals or entities. For example, in another embodiment, the GUID may be used as the password or seed for a symmetric encryption cipher known to one skilled in the art such as RC4 to generate a unique encryption key. Application of this key to the document to be signed symmetrically encrypts the document. This encrypted version of the document is unique and constitutes the signature of the document. To verify the document, either the encrypted version is decrypted using the unique key, or the presented version for verification is re-encrypted using the unique key. If the presented document is genuine, the two end products will be identical. As the GUID contains also information about the identity of the signer, an electronic signature is created. As an intermediate step in the signature process, the document may optionally be hashed or digested prior to encryption with the symmetric cipher.

Serial Number:09/081,872 [Messing] GAU 2767 Substitute Specification Mark Up 12

Thus the scope of the invention should be determined by the appended claims and their legal equivalents, rather than by the examples given. to MPEP 707.07(j).

Very respectfully,



John H. Messing
Applicant Pro Se

6571 N. Silver Smith Place, Tucson, AZ 85750
Tel.: (520) 327-7750 or (520) 529-3275

Fax: (520) 325-1087